## AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method of providing data from a service to a client over a telecommunication network based on encryption capabilities of the client, the method comprising the computer-implemented steps of:

at an intermediate server, creating and storing a mapping that associates encryption types to a plurality of available online services, wherein each of the plurality of online services is provided by one or more of a plurality of servers;

wherein the intermediate server is coupled to the client and to the plurality of servers;

at the intermediate server, receiving from the client a request for data and a list of encryption types representing encryption capabilities that are available at the client;

determining an encryption type match by matching the list of encryption types received from the client ~~list of encryption types~~ to [[a]] the mapping of encryption types to ~~a list of one or more available~~ the plurality of online services;

selecting, from the plurality of online services, an online service that can provide the data to the client[[,]] based on the encryption type match ~~and the list of one or more available online services associated with the encryption type match~~, wherein selecting the online service comprises selecting a particular server from the plurality of servers that provides the online service; and

causing communication of the data from the selected online service to the client.

2. (Original) A method as recited in Claim 1, further comprising the step of establishing a secure connection with the client, and wherein the receiving step is carried out as part of the establishing step.

3. (Original) A method as recited in Claim 1, further comprising the step of establishing a secure connection with the client, and wherein the receiving step is carried out as part of the establishing step, wherein the secure connection is established using a security protocol selected from among the set consisting of SSL, PPTP, SSH, and IPSec.

4. (Previously Presented) A method as recited in Claim 1, further comprising the step of establishing a secure connection with the client, and wherein the receiving step is carried out as part of the establishing step, wherein the step of establishing the secure connection further comprises the step of establishing the secure connection with the client using a cipher suite match.

5. (Original) The method as recited in Claim 1, further comprising the step of establishing a secure connection with the client, and wherein the receiving step is carried out as part of the establishing step, and further comprising the step of disconnecting the secure connection and reestablishing the secure connection using a cipher suite match.

6. (Currently Amended) The method as recited in Claim 1, wherein the ~~ordered~~ mapping of encryption types to services is an ordered mapping of cipher suites to services.

7. (Original) The method as recited in Claim 1, further comprising the steps of receiving a weight value for one or more of the encryption types, and ordering the mapping of encryption types to services based on the received weight values.

8. (Original) A method as recited in Claim 1, wherein the encryption type is a cipher suite match.

9. (Currently Amended) A method as recited in Claim 1, wherein the step of selecting an online service that can provide the data to the client[[,]] based the encryption type match ~~and the list of one or more available online services associated with the encryption type match~~ further comprises the step[[s]] of[[:]]

selecting a server farm based on the online service, wherein the server farm includes the plurality of servers; ~~and~~

~~selecting a particular server in the server farm to provide the data to the client~~.

10. (Original) A method as recited in Claim 1, wherein the step of causing communication further comprises the step of establishing a connection with a non-encrypted protocol for use in communicating a request to the selected service to cause communication of the data from the selected service to the client.

11. (Currently Amended) A method of providing data from a service to a client based on encryption capabilities of the client, the method comprising the computer-implemented steps of:

at an intermediate server, receiving an ordered mapping of cipher suite names to a plurality of services, wherein each of the plurality of services is provided by one or more of a plurality of servers in a server farm;

wherein the intermediate server is coupled to the client and to the plurality of servers in the server farm;

at the intermediate server, receiving from the client a request for data and an ordered list of cipher suites;

determining a cipher suite match by selecting a first common cipher suite in the ordered list of cipher suites and the ordered mapping of cipher suite names to services;

transmitting the cipher suite match to the client;

selecting, from the plurality of services, the service that is associated with the cipher suite match in the ordered mapping;

selecting [[a]] the server farm based on the service;

selecting a particular server from the plurality of servers in the server farm to provide the data to the client, wherein the particular server provides the service; and

transmitting the data to the client.

12. (Original) A method as recited in Claim 1, wherein the mapping of encryption types to services is stored in an SSL termination module.

13. (Currently Amended) A method of providing data associated with a service to a client over a telecommunication network based on SSL encryption capabilities of the client, the method comprising the computer-implemented steps of:

creating and storing, at an SSL termination device, a mapping that associates cipher suites that are supported by the SSL termination device with ~~one or more~~ a plurality of online services that are accessible through the SSL termination device, wherein each of the plurality of services is provided by one or more of a plurality of servers;

wherein the SSL termination device is coupled to the client and to the plurality of servers;

receiving from the client as part of an SSL handshake phase message, a request for data and a list of cipher suites that are available at the client;

matching the cipher suite list received from the client to the mapping to result in identifying at least one cipher suite in common between the cipher suite list and the mapping;

~~identifying, from~~ based at least on the mapping, selecting an online service from the plurality of online services that correspond[[ing]]s to the cipher suite in common, wherein selecting the online service comprises selecting a particular server from the plurality of servers that provides the online service; and

causing communication of the data from the selected online service to the client over an SSL connection using encryption parameters as defined in the cipher suite in common.

14-20. (Canceled)

21. (Canceled)

22. (Currently Amended) A computer-readable medium carrying one or more sequences of instructions for providing data from a service to a client based on encryption capabilities

of the client, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

at an intermediate server, creating and storing a mapping that associates encryption types to a plurality of available online services, wherein each of the plurality of online services is provided by one or more of a plurality of servers;

wherein the intermediate server is coupled to the client and to the plurality of servers;

at the intermediate server, receiving from the client a request for data and a list of encryption types representing encryption capabilities that are available at the client;

determining an encryption type match by matching the list of encryption types received from the client ~~list of encryption types~~ to [[a]] the mapping of encryption types to ~~a list of one or more available~~ the plurality of online services;

selecting, from the plurality of online services, an online service that can provide the data to the client[[,]] based on the encryption type match ~~and the list of one or more available online services associated with the encryption type match~~, wherein selecting the online service comprises selecting a particular server from the plurality of servers that provides the online service; and

causing communication of the data from the selected online service to the client.

23-24. (Canceled)

25. (Currently Amended) An apparatus for providing data from a service to a client based on encryption capabilities of the client, comprising:

means for executing an intermediate server that is operable to connect to the client and to a plurality of servers;

means for creating and storing, at the intermediate server, a mapping that associates encryption types to a plurality of available online services, wherein each of the plurality of online services is provided by one or more of the plurality of servers;

means for receiving from the client a request for data and a list of encryption types representing encryption capabilities that are available at the client;

means for determining an encryption type match by matching the list of encryption types received from the client ~~list of encryption types~~ to [[a]] the mapping of encryption types to ~~a list of one or more available~~ the plurality of online services;

means for selecting, from the plurality of online services, an online service that can provide the data to the client[[,]] based on the encryption type match ~~and the list of one or more available online services associated with the encryption type match~~, wherein the means for selecting the online service comprise means for selecting a particular server from the plurality of servers that provides the online service; and

means for causing communication of the data from the selected service to the client.

26. (Currently Amended) An apparatus for providing data from a service to a client based on encryption capabilities of the client, comprising:

a network interface that is coupled to a data network for receiving one or more packet flows therefrom;

a processor;

an intermediate server which, when executed by the processor, is operable to connect to the client and to a plurality of servers; and

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

creating and storing, at the intermediate server, a mapping that associates encryption types to a plurality of available online services, wherein each of the plurality of online services is provided by one or more of the plurality of servers;

receiving from the client a request for data and an ordered list of encryption types;

determining an encryption type match by matching the list of encryption types received from the client ~~list of encryption types~~ to [[a]] the mapping of

encryption types to ~~a list of one or more available~~ the plurality of online services;

determining a particular server from the plurality of servers to retrieve the data based on the encryption type match ~~and the list of one or more available online services associated with the encryption type match~~, wherein the particular server provides the service which is selected from the plurality of online services; and

causing communication of the data from the particular server to the client.

27. (Canceled)

28. (Canceled)

29. (New) An apparatus as recited in Claim 26, wherein the one or more stored sequences of instructions further comprise instructions which, when executed by the processor, cause the processor to carry out the step of establishing a secure connection with the client, and wherein the receiving step is carried out as part of the establishing step.

30. (New) An apparatus as recited in Claim 26, wherein the one or more stored sequences of instructions further comprise instructions which, when executed by the processor, cause the processor to carry out the step of establishing a secure connection with the client, and wherein the receiving step is carried out as part of the establishing step, wherein the secure connection is established using a security protocol selected from among the set consisting of SSL, PPTP, SSH, and IPSec.

31. (New) An apparatus as recited in Claim 26, wherein the one or more stored sequences of instructions further comprise instructions which, when executed by the processor, cause the processor to carry out the step of establishing a secure connection with the client, and wherein the receiving step is carried out as part of the establishing step, wherein the step of establishing the secure connection further comprises the step of establishing the secure connection with the client using a cipher suite match.

32. (New) An apparatus as recited in Claim 26, wherein the one or more stored sequences of instructions further comprise instructions which, when executed by the processor, cause the processor to carry out the step of establishing a secure connection with the client, and wherein the receiving step is carried out as part of the establishing step, and further comprising the step of disconnecting the secure connection and reestablishing the secure connection using a cipher suite match.

33. (New) An apparatus as recited in Claim 26, wherein the mapping of encryption types to services is an ordered mapping of cipher suites to services.

34. (New) An apparatus as recited in Claim 26, wherein the one or more stored sequences of instructions further comprise instructions which, when executed by the processor, cause the processor to carry out the steps of receiving a weight value for one or more of the encryption types, and ordering the mapping of encryption types to services based on the received weight values.

35. (New) An apparatus as recited in Claim 26, wherein the encryption type is a cipher suite match.

36. (New) An apparatus as recited in Claim 26, wherein the instructions that cause the processor to carry out the step of selecting an online service that can provide the data to the client based the encryption type match further comprise instructions which, when executed by the processor, cause the processor to carry out the step of selecting a server farm based on the online service, wherein the server farm includes the plurality of servers.

37. (New) An apparatus as recited in Claim 26, wherein the instructions that cause the processor to carry out the step of causing communication further comprise instructions which, when executed by the processor, cause the processor to carry out the step of establishing a connection with a non-encrypted protocol for use in communicating a request

to the selected service to cause communication of the data from the selected service to the client.

38. (New) An apparatus as recited in Claim 26, further comprising an SSL termination module that is operable to store the mapping of encryption types to services.

39. (New) An apparatus as recited in Claim 25, further comprising means for establishing a secure connection with the client, wherein the means for establishing the secure connection include the means for receiving the request from the client.

40. (New) An apparatus as recited in Claim 25, further comprising means for establishing a secure connection with the client, wherein the means for establishing the secure connection include the means for receiving the request from the client, wherein the secure connection is established using a security protocol selected from among the set consisting of SSL, PPTP, SSH, and IPSec.

41. (New) An apparatus as recited in Claim 25, further comprising means for establishing a secure connection with the client, wherein the means for establishing the secure connection include the means for receiving the request from the client, wherein the means for establishing the secure connection further comprise means for establishing the secure connection with the client using a cipher suite match.

42. (New) An apparatus as recited in Claim 25, further comprising:

means for establishing a secure connection with the client, wherein the means for establishing the secure connection include the means for receiving the request from the client; and

means for disconnecting the secure connection and reestablishing the secure connection using a cipher suite match.

43. (New) An apparatus as recited in Claim 25, wherein the mapping of encryption types to services is an ordered mapping of cipher suites to services.

44. (New) An apparatus as recited in Claim 25, further comprising means for receiving a weight value for one or more of the encryption types and means for ordering the mapping of encryption types to services based on the received weight values.

45. (New) An apparatus as recited in Claim 25, wherein the encryption type is a cipher suite match.

46. (New) An apparatus as recited in Claim 25, wherein the means for selecting an online service that can provide the data to the client based the encryption type match further comprise means for selecting a server farm based on the online service, wherein the server farm includes the plurality of servers.

47. (New) An apparatus as recited in Claim 25, wherein the means for causing communication further comprise means for establishing a connection with a non-encrypted protocol for use in communicating a request to the selected service to cause communication of the data from the selected service to the client.

48. (New) An apparatus as recited in Claim 25, further comprising an SSL termination module that is operable to store the mapping of encryption types to services.

49. (New) An apparatus for providing data from a service to a client based on encryption capabilities of the client, comprising:

means for executing an intermediate server that is operable to connect to the client and to a plurality of servers in a server farm;

means for receiving an ordered mapping of cipher suite names to a plurality of services, wherein each of the plurality of services is provided by one or more of the plurality of servers in the server farm;

means for receiving from the client a request for data and an ordered list of cipher suites;

means for determining a cipher suite match by selecting a first common cipher suite in the ordered list of cipher suites and the ordered mapping of cipher suite names to services;

means for transmitting the cipher suite match to the client;

means for selecting, from the plurality of services, the service that is associated with the cipher suite match in the ordered mapping;

means for selecting the server farm based on the service;

means for selecting a particular server from the plurality of servers in the server farm to provide the data to the client, wherein the particular server provides the service; and

means for transmitting the data to the client.

50. (New) An apparatus for providing data from a service to a client over a telecommunication network based on Secure Socket Layer (SSL) encryption capabilities of the client, comprising:

an SSL termination device that is operable to connect to the client and to a plurality of servers;

means for creating and storing, at the SSL termination device, a mapping that associates cipher suites that are supported by the SSL termination device with a plurality of online services that are accessible through the SSL termination device, wherein each of the plurality of services is provided by one or more of the plurality of servers;

means for receiving from the client as part of an SSL handshake phase message, a request for data and a list of cipher suites that are available at the client;

means for matching the cipher suite list received from the client to the mapping to result in identifying at least one cipher suite in common between the cipher suite list and the mapping;

means for selecting, based at least on the mapping, an online service from the plurality of online services that corresponds to the cipher suite in common, wherein the means for selecting the online service comprise means for

selecting a particular server from the plurality of servers that provides the online service; and

means for causing communication of the data from the selected online service to the client over an SSL connection using encryption parameters as defined in the cipher suite in common.